MEGAMIND
Research on Usability in Information Security

E. Eugene Schultz, Ph.D., CISSP, CISM

Introduction

Usability engineering, often also called human factors engineering, focuses on optimizing the interaction between humans and the tasks they perform. Given the long-recognized importance of usability engineering in areas such as human-computer interaction, it is easy to assume that a plethora of research on the relationship between usability and information security exists. Strangely, the opposite is the case. Although numerous authors have argued for the need to pay more attention to usability considerations in information security, relatively few papers presenting research results on the relationship between usability and information security have been published. This paper covers several key research papers on this topic.

Whitten and Tygar (1999)—Usability Problems in PGP 5.0

Whitten and Tygar published what appears to be the first research study on the relationship between usability and information security when they performed usability analysis and testing on version 5.0 of PGP (Pretty Good Privacy), a tool for encrypting and digitally signing email (WHIT99). PGP is widely used, and according to these researchers, it has a user interface that by general standards is easy to use. The study involved only users who were naïve with respect to cryptography; their task was to use PGP to encrypt, digitally sign, and send email. A walkthrough analysis of users' interactions with this tool revealed numerous user interface design weaknesses that appeared to increase the tendency of users to make errors. Users were also allocated 90 minutes to sign and encrypt a message using PGP 5.0; the majority was unable to do so successfully. Whitten and Tygar concluded that even though PGP 5.0 has an attractive graphical user interface, for most users this tool is not sufficiently usable to be effective from a security perspective. They stated that user interface design in security-related user interaction tasks is deficient; interfaces used in interaction tasks related to information security are in general "clumsy, confusing, or near-nonexistent." Different usability standards, ones that are specifically applicable to information security, need to be developed accordingly.

Proctor et al. (2000)—Usability Problems in Third-Party Authentication Methods

Proctor et al. performed and published research on usability considerations in third-party authentication methods (PROC00). This research was in part motivated by growing dissatisfaction with the use of password-based authentication. Passwords are highly vulnerable to being guessed, cracked, and revealed by users; third-party authentication methods such as biometric- and smart card-based authentication are increasingly being touted as better alternatives. These researchers performed task analyses, decomposing users' tasks into individual, sequential steps or elements to analyze the relative complexity of each task, to determine the number of task steps involved in biometric, smart card and password authentication. In general, the more steps involved in a task, the more difficult that task is to perform. Not only do tasks that involve a greater number of steps tend to increase the time needed to perform them, but they also tend to produce more user errors. Both the biometric and smart card methods utilized devices that were frequently used and widely available. The researchers found that compared to password authentication, biometric devices required 10 additional task steps. Smart cards were even worse in that compared to password authentication, 14 additional task steps were required. Results suggest an explanation concerning why third-party authentication methods have not gained in popularity as much as security needs would appear to dictate. Having to perform numerous additional steps in third-party authentication presents a significant usability hurdle to users, one that in all likelihood produces a great deal of user frustration and ultimately resistance to this type of authentication. Additionally, some of the steps identified in the task analyses were considerably more likely to produce user errors than others. For example, inserting a smart card correctly into the card reader comprised a series of steps that required precisely orienting and manipulating the smart card such that it could be inserted directly into the reader, something that could easily result in errors on the part of users. Finally, the results of the task analyses suggest that not all third-party authentication methods are equally conducive to usability—biometric authentication turned out to be less extensive in terms of steps needing to be performed than did smart card authentication. The authors concluded that information security managers and staff should include usability considerations in the many cost-benefit tradeoffs involving security controls and countermeasures.

Wool—Usability Problems in Firewalls

Wool's research focused on usability problems in frequently used firewall products. Firewalls can be configured to selectively filter traffic on the basis of packet header information such as source and destination IP address, source and destination port, type of protocol, and other information,. Other parameters that can be used in filtering traffic include the particular network interface card each packet crosses and whether each packet crosses the interface from outside of the network into the firewall or in the opposite direction. Access rules for inbound traffic are often different from those for outbound traffic. Anti-spoofing rules, for example, are based on the fact that no inbound traffic should have the source IP address of any internal host. Packet direction is thus very useful in configuring firewall rules. Lamentably, directionality is from a firewall configuration perspective typically different from users' expectations. If an interface connects a firewall to an internal network, the firewall treats the traffic as outbound (from the interface), whereas most users would view the traffic as inbound. In most firewalls the user interface conventions concerning traffic direction are designed from the perspective of a firewall, not a user point of view. Configuring a firewall correctly can thus be a daunting task, one that is anything but user friendly. The RADIS algorithm within a prototype Wool calls Firmato provides a solution—firewall management software actually computes each direction of traffic for firewalls placed on the perimeter of networks. Firmato's input comes from the security policy that someone specifies as well as the network topology covered by the policy. This information is written in Firmato's model description language (MDL). A compiler parses MDL input, uses several phases of compilation to transform the data, and yields firewall rules written in the language of the particular firewall in question. The RADIS algorithm is applied immediately before rules are translated into a firewall's language. Input to the RADIS algorithm consists of the rulebase, the complete list of rules that comprise the security policy, and the description of the network topology, which includes the yet unconfigured firewalls, the associated interfaces and IP addresses of each, and the subnets behind each. Each rule contains fields such as IP addresses, protocol types, and port numbers, but does not specify directions for traffic. The network topology description includes a listing of the firewalls that need to be configured, each of which is listed with all of its interfaces and IP addresses. In addition, the description lists the complete set of IP addresses and subnets that are located behind each firewall interface. The RADIS algorithm then creates a graph of the network, setting the direction field of each rule by posing the question "could rule r possibly ever be relevant to a non-spoofed packet trying to pass through interface i in direction d" expressed in graph theoretic terms. The question can be answered by locating the network zones in which the rule's source and destination reside and then computing the path between them across the firewall. RADIS ultimately creates firewall configurations that provide protections specified in the security policy that include appropriate directionality without firewall administrators being aware of how this is being done.

Vu et al.—Password memorability and resistance to cracking are inversely related

Vu and several other researchers conducted multiple studies to determine whether having users create sentences and then use the first letters of each word in the sentences to form passwords would improve password recall as well as resistance to cracking (VU04). Results showed that creating sentences yielded more crack-resistant passwords only when users were told to embed a digit and special character into the sentence (and thus also in the password). Embedding a digit and special character also resulted in less ability to remember passwords when users were tested for both short-term and long-term recall, however. Additionally, embedding digits and special characters resulted in more time needed to generate passwords. These results cast doubt on recommendations to use passphrases to improve password memorability and resistance to cracking. Creating sentences in and of itself made little difference. In contrast, embedding a digit and special character into passwords derived from sentences improved resistance to password cracking, but memorability declined, showing that under the conditions investigated in these studies there is a tradeoff between choosing passwords that are resistant to cracking and password memorability. Security and usability were in this case orthogonal to each other.

Conclusion

The research studies summarized in this paper by no means are representative the totality of research conducted on the relationship between usability and human factors, but at the same time it is important to realize that relatively little research on this relationship has been performed so far. For the most part these studies show that usability problems exist in tasks involving information security; some of them are severe. Whitten and Tygar’s research was important in first helping make the information security community aware that there are numerous usability problems in the use of cryptography. Proctor et al.’s research showed that although stronger authentication methods than password-based authentication are available, some of these methods present significant usability hurdles in that they require numerous additional task steps. Wool pointed out some of the usability problems associated with configuring firewalls to selectively filter traffic and developed a solution that improves usability by providing among other things a graphical representation of the network topology and rules for controlling traffic that flows within it. Vu et al. showed that passwords derived from sentences do not necessarily improve both password security and memorability. All of these studies point to the need to pay much closer attention to human factors in information security-related tasks.

References

PROC00 Proctor, Robert W., Lien, Mei-Ching, Salvendy, Gavriel, & Schultz, E. Eugene, A task analysis of usability in third-party authentication. Information Security Bulletin, 5 (3), April 2000, pp. 49 – 56.

VU04 Vu, Kim-Phuong L., Tai, Bik-Lam, Bhargav, Abhilasha, Schultz, E. Eugene & Proctor, Robert W., Promoting memorability and security of passwords through sentence generation. Proceedings of the Human Factors and Ergonomics Society's 48th Annual Meeting, September 2004.

WHIT99 Whitten, Alma & Tygar, J.D., Why Johnny can't encrypt: A usability evaluation of PGP 5.0. 8th USENIX Security Symposium, August 1999.

WOOL04 Wool, Avishai, The use and usability of direction-based filtering in firewalls. Computers & Security, Volume 23 (6), September 2004, pp. 459-468.